



Relativistic Causality vs No-Signalling

Ravishankar Ramanathan

The University of Hong Kong

joint work with Pawel Horodecki,
National Quantum Information Centre, University of Gdansk

P. Horodecki and R. Ramanathan. “*The relativistic causality versus no-signalling paradigm for multi-party correlations*”. *Nature Communications* 10, 1701 (2019).



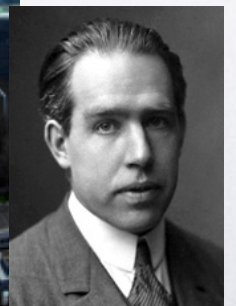
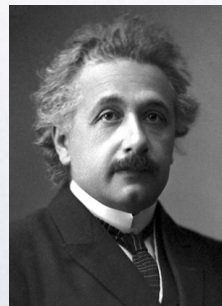
Outline

- Multi-party No-Signaling constraints $\neq$ constraints imposed by Relativistic Causality.
- Constraints depend on spacetime coordinates of measurement events $P((t_1, r_1), \dots, (t_n, r_n))(a_1, \dots, a_n | x_1, \dots, x_n)$.
- Implications:
 - Device-Independent cryptography against relativistically constrained adversaries; new Free-Will in Bell Theorem.
 - Multi-party non-locality; lack of monogamy of non-local correlations.
 - Proofs showing quantum correlations cannot arise from finite speed v -causal models look incomplete.



Bell Non-Locality

- **Bell Non-locality:** *There exist correlations between space-like separated events that violate Bell inequalities.*
- Nature does not obey a notion of ‘*Local Causality*’
- At least one of the intuitive notions of *determinism, statistical locality or measurement independence* seems to be in conflict with experiment.

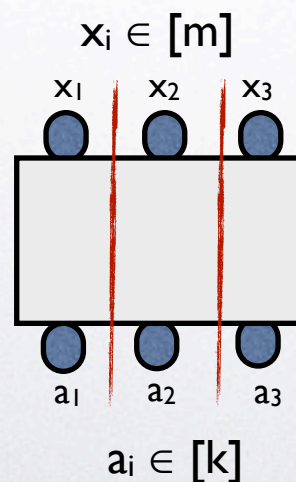




Bell Experiment: Setup

- Bell experiment. Scenario $B(n,m,k)$: n parties, m settings and k outcomes.
- Preparation procedure Q . Measurement procedure $(x_1, \dots, x_n)$. Outcome $(a_1, \dots, a_n)$. Underlying variables λ .

$$P(a_1, a_2 | x_1, x_2, Q) = \int d\lambda P(a_1, a_2 | x_1, x_2, Q, \lambda) P(\lambda | x_1, x_2, Q)$$



$$P_q(a_1, a_2 | x_1, x_2, Q, \lambda) = \text{tr} [\lambda E_{a_1}^{x_1} \otimes E_{a_2}^{x_2}] .$$

λ : density operator ρ in QM

$$P(\lambda | x, P) = \delta(\lambda - \rho)$$

Box: $P(a_1, a_2, a_3 | x_1, x_2, x_3)$

I. Pitowsky, Quantum Probability - Quantum Logic, Springer-Verlag Vol. 321 (1989).

A. Peres, Foundations of Physics 29(4) 589 (1999).



Bell inequalities: Assumptions

- Assumptions in deriving Bell inequalities:
 - **Statistical Completeness/Outcome Independence:** All statistical correlations arise from ignorance of the underlying variable λ

$$P(a_1, a_2 | x_1, x_2, Q, \lambda) = P(a_1 | x_1, x_2, Q, \lambda) P(a_2 | x_1, x_2, Q, \lambda)$$

- True for deterministic models. Motivation: Underlying reality with measurement outcomes predetermined.



- **Statistical Locality/Parameter Independence/No-Signaling:** Distant measurements do not influence a party's underlying outcome prob. dist.

$$\begin{aligned} P(a_1 | x_1, x_2, Q, \lambda) &= P(a_1 | x_1, Q, \lambda), \\ P(a_2 | x_1, x_2, Q, \lambda) &= P(a_2 | x_2, Q, \lambda). \end{aligned}$$

- Justification comes from Special Relativity when measurements are spacelike separated.



Bell Inequalities: Assumptions

- Assumptions in deriving Bell inequalities:



- **Measurement Independence/Free-Will:** Measurement inputs (x_1, x_2) are uncorrelated with the underlying variable λ .

$$P(\lambda|x_1, x_2, Q) = P(\lambda|Q).$$

- **Reality is single valued, Fair Sampling, No Backward Causation, etc.**

- Putting it all together, we obtain the Local Hidden Variable (LHV) model:

$$P(a_1, a_2|x_1, x_2, Q) = \int d\lambda P(\lambda|Q)P(a_1|x_1, \lambda, Q)P(a_2|x_2, \lambda, Q).$$



No-Signalling

- One can ‘deduce’ the no-signalling constraints from the assumptions of measurement independence and parameter independence

$$\begin{aligned} P_{A_1|X_1, X_2}(a_1|x_1, x_2) &= \int d\lambda P_{\Lambda|X_1, X_2}(\lambda|x_1, x_2) P_{A_1|X_1, X_2, \Lambda}(a_1|x_1, x_2, \lambda) \\ &\stackrel{\text{Eq. (5)}}{=} \int d\lambda P_{\Lambda}(\lambda) P_{A_1|X_1, X_2, \Lambda}(a_1|x_1, x_2, \lambda) \\ &\stackrel{\text{Eq. (4)}}{=} \int d\lambda P_{\Lambda}(\lambda) P_{A_1|X_1, \Lambda}(a_1|x_1, \lambda) \\ &= P_{A_1|X_1}(a_1|x_1). \\ P_{A_2|X_1, X_2}(a_2|x_1, x_2) &= \int d\lambda P_{\Lambda|X_1, X_2}(\lambda|x_1, x_2) P_{A_2|X_1, X_2, \Lambda}(a_2|x_1, x_2, \lambda) \\ &\stackrel{\text{Eq. (5)}}{=} \int d\lambda P_{\Lambda}(\lambda) P_{A_2|X_1, X_2, \Lambda}(a_2|x_1, x_2, \lambda) \\ &\stackrel{\text{Eq. (4)}}{=} \int d\lambda P_{\Lambda}(\lambda) P_{A_2|X_2, \Lambda}(a_2|x_2, \lambda) \\ &= P_{A_2|X_2}(a_2|x_2). \end{aligned}$$



Motivation for parameter independence: Causality

- As usual in Bell non-locality, let us work within the classical spacetime of Special Relativity.
- **Causality**: No causal loops. i.e. *No faster-than-light transmission of information from one spacetime location to another space-like separated location.*
- Causality violated if an effect at spacetime location A precedes its cause at spacetime location B ($t_A < t_B$) in some inertial reference frame.



Correlation is not causation!

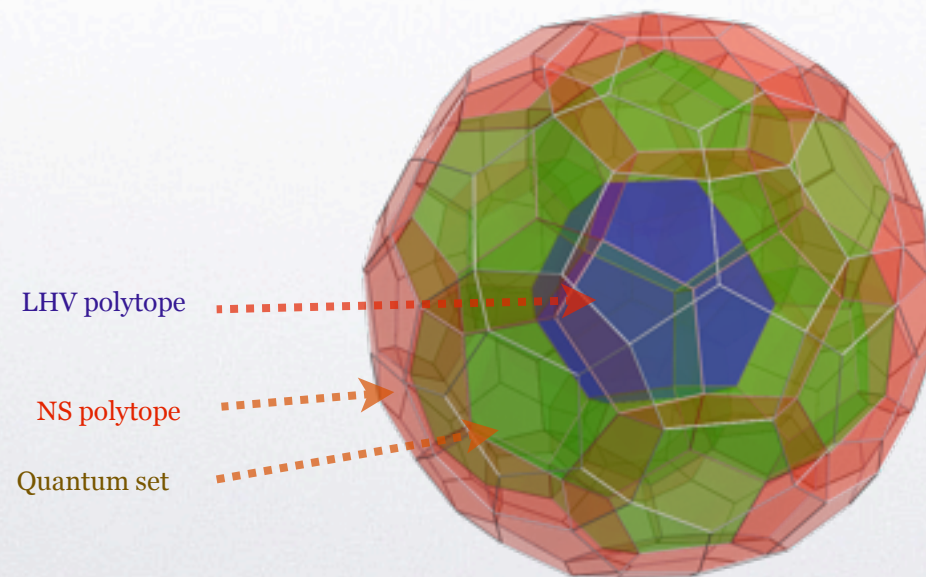


No-Signaling Polytope

- Box: Set of cond. prob. dist. $P(\mathbf{a}|\mathbf{x}) = P(a_1, \dots, a_n | x_1, \dots, x_n)$.
- Non-negativity: $P(\mathbf{a}|\mathbf{x}) \geq 0$. Normalization: $\sum_{\mathbf{a}} P(\mathbf{a}|\mathbf{x}) = 1$.
- Multi-party No-Signaling (Directly generalize from the two-party case):

$$\sum_{a_j} P(a_1, \dots, a_j, \dots, a_n | x_1, \dots, x_j, \dots, x_n) = \sum_{a_j} P(a_1, \dots, a_j, \dots, a_n | x_1, \dots, x'_j, \dots, x_n) \quad \forall j, x_j, x'_j, \mathbf{a} \setminus a_j, \mathbf{x} \setminus x_j.$$

- LHV polytope $\subset$ Quantum Correlations $\subset$ No-Signaling Polytope



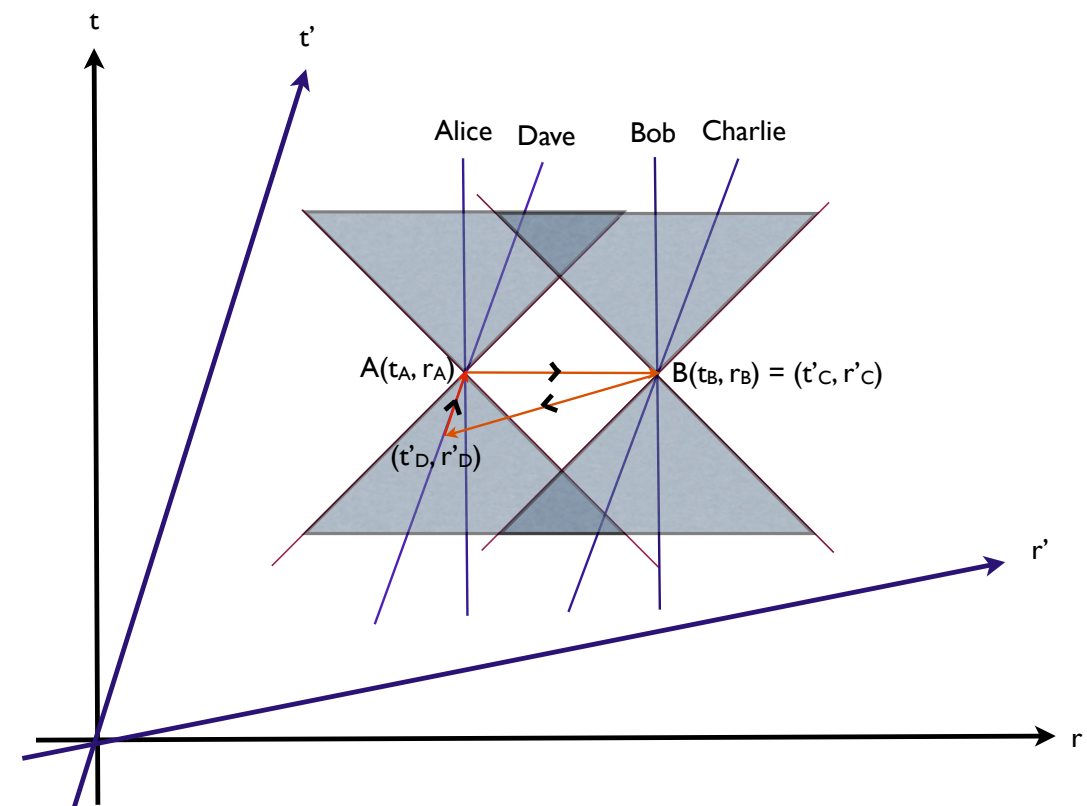
Consequence of causality?



Two-party No-Signaling from Relativistic Causality

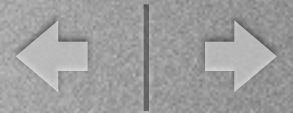
- Formalism: Spacetime Random Variable (**strv** = **r.v. generated at spacetime location $(t, \mathbf{r})$**).
- Alice inputs x , obtains output a (instantaneously) at spacetime location A.
- Bob inputs y , obtains output b (instantaneously) at spacetime location B.
- FreeWill + Causality $\Rightarrow$ NoSignaling.

$$P(a_1|x_1, x_2, Q, \lambda) = P(a_1|x_1, Q, \lambda),$$
$$P(a_2|x_1, x_2, Q, \lambda) = P(a_2|x_2, Q, \lambda).$$



R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450-454 (2012).

P. Horodecki and R. R., *in preparation*. P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)



Multi-party No-Signaling from Relativistic Causality

- Spacetime rv's: Alice's measurement input-output rv's (x,a) at spacetime location A, Bob's (y,b) at B, Charlie's (z,c) at C.

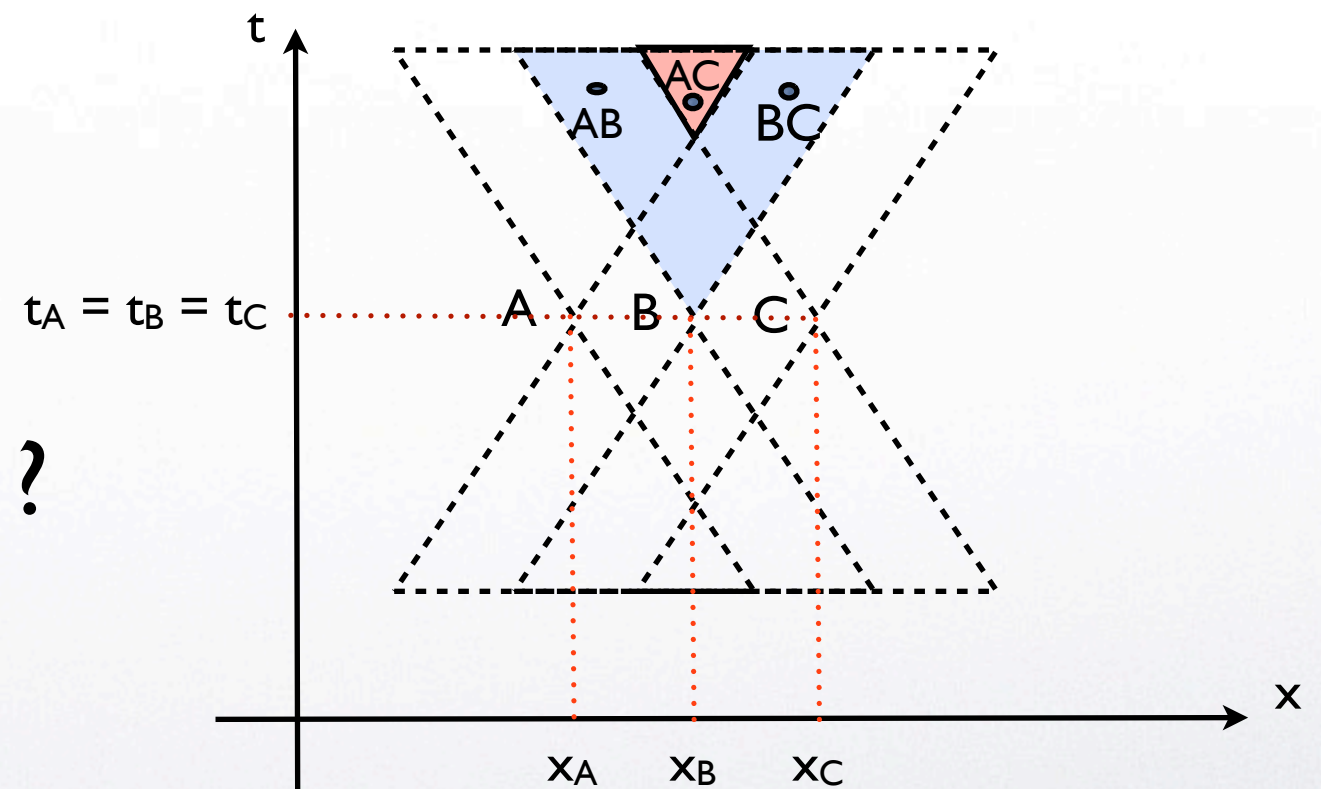
- No-Signaling:

$$\sum_c P(a,b,c|x,y,z) = \sum_c P(a,b,c|x,y,z') \quad \forall z,z',a,b,x,y$$

$$\sum_b P(a,b,c|x,y,z) = \sum_b P(a,b,c|x,y',z) \quad \forall y,y',a,c,x,z \quad ?$$

$$\sum_a P(a,b,c|x,y,z) = \sum_a P(a,b,c|x',y,z) \quad \forall x,x',b,c,y,z.$$

- AB output marginal independent of C's input.
AC output marginal independent of B's input.
BC output marginal independent of A's input.
- A, B, C individual marginals well-defined.



Notice that intersection of future light cones of A and C is contained within the future light cone of B

J. Grunhaus, S. Popescu and D. Rohrlich, Phys. Rev. A 53, 3781 (1996).

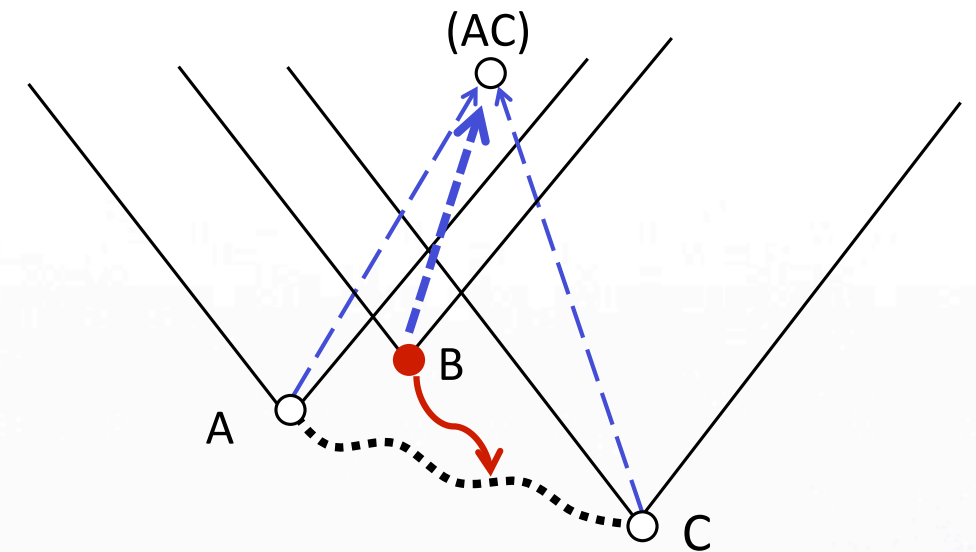
S. Popescu and D. Rohrlich, Non-Locality as an axiom for quantum theory, arXiv:9508009 (1995).

P. Horodecki and R. R., *in preparation*. P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)



Multi-party No-Signaling from Relativistic Causality

- **Observation:** Alice and Bob check correlations at spacetime location AB (the correlations give rise to the spacetime variable AB at this location). Similarly, Alice-Charlie at AC as well as Bob-Charlie at BC.
- **Argument:** Suppose a (superluminal) influence propagates from B to AC, changing the correlations AC while keeping marginals A and C fixed.
- **Proof:** shows that such a influence does not lead to any causal loops.



- **Justification:** Spacetime random variable AC representing correlations is only registered at a point located within the future light cone of B. It means that effectively information has been sent from B to its future which ensures no causal loops.



Modified Multi-party No-Signaling from Relativistic Causality

- Modified 3-party constraints that prevent causality violations (when Bob is in appropriate space-time region):

$$\begin{aligned}\sum_c P(a, b, c | x, y, z) &= \sum_c P(a, b, c | x, y, z') \quad \forall z, z', a, b, x, y \\ \sum_a P(a, b, c | x, y, z) &= \sum_a P(a, b, c | x', y, z) \quad \forall x, x', b, c, y, z \\ \sum_{a,b} P(a, b, c | x, y, z) &= \sum_{a,b} P(a, b, c | x', y', z) \quad \forall x, x', y, y', c, z \\ \sum_{b,c} P(a, b, c | x, y, z) &= \sum_{b,c} P(a, b, c | x, y', z') \quad \forall y, y', z, z', a, x.\end{aligned}$$

- In general, in the n-party scenario (for a 1-D spatial arrangement of parties): Let $S_{m,k}^n$ denote a contiguous subset of $[n]$ with initial element m and size k .

$$P(\mathbf{a}_{S_{m,k}^n} | \mathbf{x}_{S_{m,k}^n}) = \sum_{\mathbf{a}'_{(S_{m,k}^n)^c}} P(\mathbf{a}' | \mathbf{x}') = \sum_{\mathbf{a}''_{(S_{m,k}^n)^c}} P(\mathbf{a}'' | \mathbf{x}'') \quad \forall 1 \leq k \leq n-1, 1 \leq m \leq n-k+1$$

for all $\mathbf{a}', \mathbf{a}''$ with $\mathbf{a}'_{S_{m,k}^n} = \mathbf{a}''_{S_{m,k}^n} = \mathbf{a}_{S_{m,k}^n}$ and for all

$\mathbf{x}', \mathbf{x}''$ with $\mathbf{x}'_{S_{m,k}^n} = \mathbf{x}''_{S_{m,k}^n} = \mathbf{x}_{S_{m,k}^n}$.

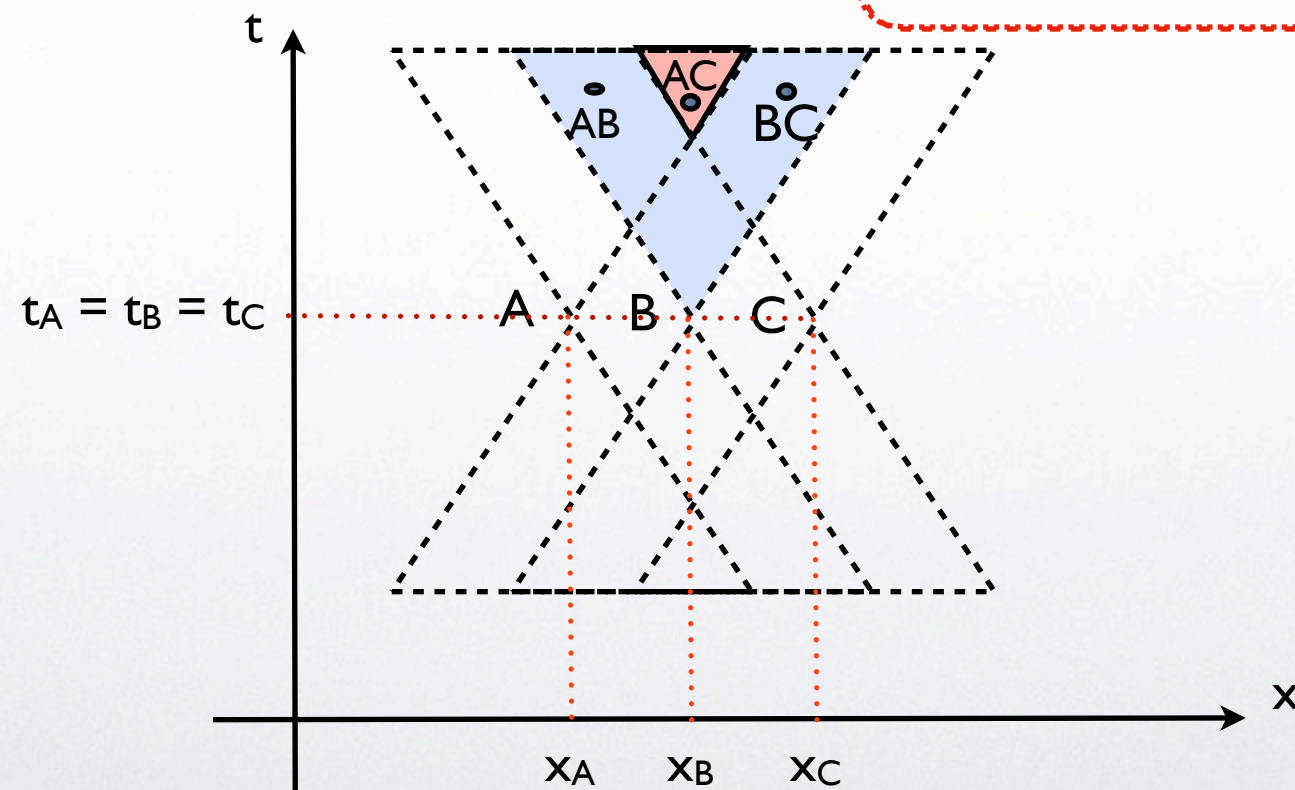


Compatibility with Free Will

- **Free-Will** conditions are intimately connected with No-Signaling constraints:

$$P(a, c|x, y, z) = \frac{P(a, c|x, z)P(y|a, c, x, z)}{P(y|x, z)}$$

$$= P(a, c|x, z) \quad \text{Free-Will: } P(y|a, c, x, z) = P(y|x, z) = P(y)$$



R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450-454 (2012).

R. Colbeck and R. Renner, A short note on the concept of free choice, arXiv: 1302.4446 (2013).



Compatibility with Free Will

- Colbeck-Renner (formalising Bell): *A spacetime random variable is free if the only variables it is correlated with are those it could have caused, i.e., those in its future light cone.*

Definition 4. We say that $A \in \Gamma$ is *free* if

$$P_{A\Gamma_A} = P_A \times P_{\Gamma_A}$$

holds, where Γ_A is the set of all RVs $X \in \Gamma$ such that $A \not\rightarrow X$.¹²

- If we modify NS constraints, should also modify free-will constraints.





Compatibility with Free-Will

- **Argument:** Correlations AC properly seen as spacetime r.v. generated in the future light cone of B.

Definition 4. Let $A_{X_i \rightarrow} = \{A_j\}$ denote a set of outputs A_j such that the correlation SRV $C_{\{A_j\}}$ between all the A_j is generated outside the future light cone of X_i . Then X_i is said to be free if the following condition is satisfied:

$$P(X_i | \mathbf{X} \setminus X_i, A_{X_i \rightarrow}, S_{P_1 \dots P_n}) = P(X_i). \quad (25)$$

- CR: No extension of quantum theory compatible with usual notion of free-will can have better predictive power (for instance, Bohmian theories).

P. Horodecki and R.R, *in preparation*. P. Horodecki and R. R. Nat. Comm. 10, 1701 (2019)

R. Colbeck and R. Renner, No extension of quantum theory can have improved predictive power, Nature Communications 2, 411 (2011).

Finite superluminal causal influences as explanations of quantum nonlocality

- Breakthrough result of Bancal et al.: A multi-party Bell experiment that shows any finite-speed v -causal model leads to signaling.
- *Under the restricted free-will/ relativistic causality constraints, in the measurement configurations considered so far, one can explain the quantum correlations by means of a v -causal model.*
- **Work in progress: Can further modified BI's rule out v -causal explanations?**

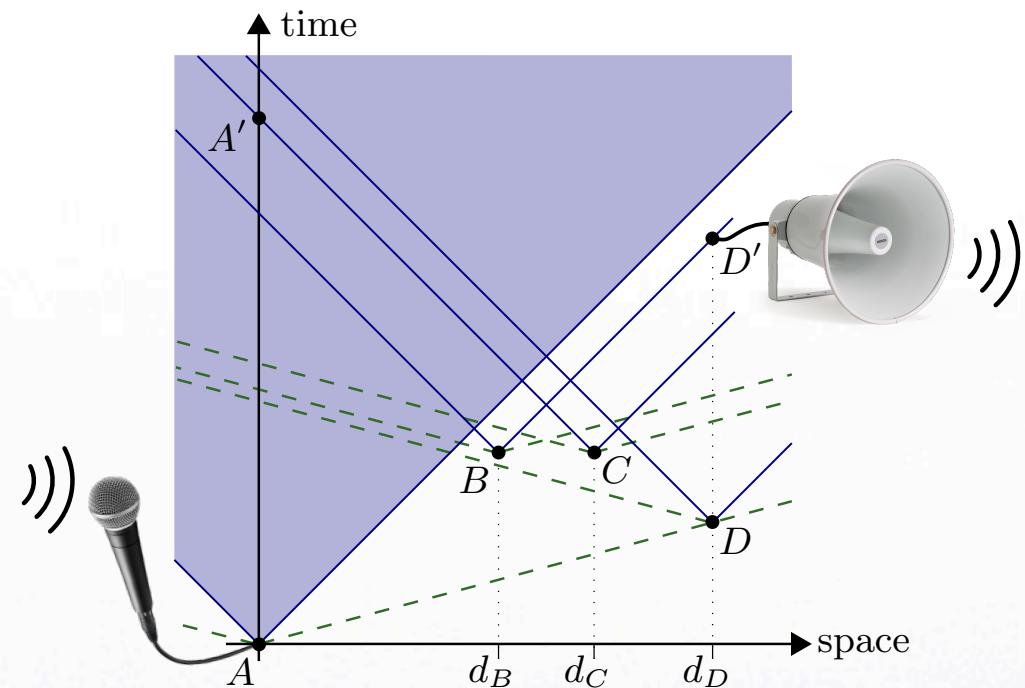


FIG. 3. Four-partite Bell-type experiment characterized by the spacetime ordering $R = (A < D < (B \sim C))$. Since B and C are both measured after A and D and satisfy $B \sim C$, the $BC|AD$ correlations produced by a v -causal model are local (see Appendix C). A violation of the inequality of Lemma 1 by the model therefore implies that the corresponding correlations must violate the no-signalling conditions (1). At least one of the tripartite correlations ABC , ABD , ACD , or BCD must then depend on the measurement setting of the remaining party. The marginal ABD (ACD) cannot depend on z (y), since this measurement setting is freely chosen at C (B), which is outside the past v -cone of A , B (C) and D (see also Appendix D). It thus follows that either the marginal ABC must depend on the measurement setting w of system D or that the marginal BCD must depend on the measurement setting x of system A (or both). Let the four systems



Quantum non-locality based on finite-superluminal influences leads to signaling

Lemma 1. *Let $P(abcd|xyzw)$ be a joint probability distribution with $a, b, c, d \in \{0, 1\}$ and $x, y, z, w \in \{0, 1\}$ satisfying the following two conditions.*

(a) *The conditional bipartite correlations $BC|AD$ are local, i.e., the joint probabilities $P(bc|yz, axdw)$ for systems BC conditioned on the measurements settings and results of systems AD admit a decomposition of the form $P(bc|yz, axdw) = \sum_{\lambda} q(\lambda|axdw)P(b|y, \lambda)P(c|z, \lambda)$ for every a, x, d, w .*

(b) *P satisfies the no-signalling conditions (1).*

Then there exist a four-partite Bell expression S (see Appendix B for its description) such that correlations satisfying (a) and (b) necessarily satisfy $S \leq 7$, while there exist local measurements on a four-partite entangled quantum state that yield $S \simeq 7.2 > 7$.

$$\begin{aligned} S = & -3\langle A_0 \rangle - \langle B_0 \rangle - \langle B_1 \rangle - \langle C_0 \rangle - 3\langle D_0 \rangle \\ & - \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle + \langle A_0 C_0 \rangle \\ & + 2\langle A_1 C_0 \rangle + \langle A_0 D_0 \rangle + \langle B_0 D_1 \rangle \\ & - \langle B_1 D_1 \rangle - \langle C_0 D_0 \rangle - 2\langle C_1 D_1 \rangle \\ & + \langle A_0 B_0 D_0 \rangle + \langle A_0 B_0 D_1 \rangle + \langle A_0 B_1 D_0 \rangle \\ & - \langle A_0 B_1 D_1 \rangle - \langle A_1 B_0 D_0 \rangle - \langle A_1 B_1 D_0 \rangle \\ & + \langle A_0 C_0 D_0 \rangle + 2\langle A_1 C_0 D_0 \rangle - 2\langle A_0 C_1 D_1 \rangle \\ & \leq 7, \end{aligned}$$

$$\begin{aligned} |\Psi\rangle = & \frac{17}{60}|0000\rangle + \frac{1}{3}|0011\rangle - \frac{1}{\sqrt{8}}|0101\rangle + \frac{1}{10}|0110\rangle \\ & + \frac{1}{4}|1000\rangle - \frac{1}{2}|1011\rangle - \frac{1}{3}|1101\rangle + \frac{1}{2}|1110\rangle. \end{aligned}$$

$$\begin{aligned} \hat{A}_0 &= -U\sigma_x U^\dagger, \quad \hat{A}_1 = U\sigma_z U^\dagger, \quad \hat{B}_0 = H, \\ \hat{B}_1 &= -\sigma_x H \sigma_x, \quad \hat{C}_0 = -\hat{D}_0 = \sigma_z, \quad \hat{C}_1 = \hat{D}_1 = -\sigma_x, \end{aligned}$$



Device-Independent crypto against Relativistic Eavesdroppers

- Boxes $P(\mathbf{a}|\mathbf{x}) = P(a_1, \dots, a_n | x_1, \dots, x_n)$ must carry a label of space-time locations of measurement events $P((t_l, r_l), \dots, (t_n, r_n))(a_1, \dots, a_n | x_1, \dots, x_n)$.
- The set of boxes $P(\mathbf{a}|\mathbf{x})$ respecting relativistic causality forms a larger dimensional polytope containing the usual NS polytope.
- LHV polytope $\subset$ Quantum Correlations $\subset$ No-Signaling Polytope $\subset$ Causality Polytope.
- In DIQKD against relativistic eavesdroppers, this gives a larger set of attack strategies for Eve.

R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450-454 (2012).

R. Gallego et al., Full randomness from arbitrarily deterministic events, Nat. Comm. 4, 2654 (2013).

F. G. S. L. Brandao, R. R. A. Grudka, Horodecki³, T. Szarek, H. Wojewodka, Nat Comm. 7, 11345 (2016).



Device-Independent Randomness Amplification against Relativistic Eve

- Randomness amplification of Santha-Vazirani sources: need BI with algebraic violation. Paradigmatic example: GHZ-Mermin inequality.
- We show that no randomness can be extracted from the settings that appear in the Mermin inequality under the new constraints, even with maximal violation.

Proposition 7. *Consider the n -party GHZ-Mermin Bell inequality, for odd $n \geq 3$. Suppose that in some inertial reference frame, the n space-like separated parties are arranged in 1-D, with $r_1 < \dots < r_n$ and perform their measurements simultaneously, i.e., $t_1 = \dots = t_n$. Then for any input $\mathbf{x}^*$ appearing in the inequality, i.e., $\mathbf{x}^* \in \mathcal{X}_{\text{Merm}}^n$, there exists a box $\mathcal{P}$ violating the Mermin inequality maximally and obeying the relativistic causality constraints in Eq.(17), such that no randomness can be extracted from the outputs $\mathbf{a}$ of the box under input $\mathbf{x}^*$. In other words, we have*

$$\mathcal{P}(\mathbf{a}^*|\mathbf{x}^*) = 1, \tag{33}$$

for some fixed output bit string $\mathbf{a}^*$.



DI Randomness Amplification against relativistic Eve

- Proof is by construction of box $P(a|x)$ that satisfies:
 - GHZ-Mermin constraints
 - Causality constraints
 - returns deterministic output for settings appearing in the inequality.

Algorithm 1 Construction of box $\mathcal{P}$

- 1: **procedure** CONSTRUCTION OF $\mathcal{P}$
- 2: Let $\mathbf{x}^* \in \mathcal{X}_{\text{Mermin}}^{n,1}$ be given. Initiate as step 0, $\mathbf{a}^l(\mathbf{x}^*) = \mathbf{a}^r(\mathbf{x}^*) = \mathbf{a}^*$ (the all-0 bit string).
- 3: At the $(2j+1)$ -th step, $0 \leq j \leq \frac{n-1}{2}, \forall 1 \leq i_1 \leq \dots \leq i_{2j+1} \leq n$, if $\mathbf{x}_{i_{2j+1}}^* = 0$ define

$$\begin{aligned} \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j+1}}) &:= \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}) \\ \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j+1}}) &:= \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}) \oplus \mathbf{1}^{i_j}. \end{aligned} \quad (46)$$

If on the other hand, $\mathbf{x}_{i_{2j+1}}^* = 1$ define

$$\begin{aligned} \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j+1}}) &:= \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}) \oplus \mathbf{1}^{i_{2j+1}} \\ \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j+1}}) &:= \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}). \end{aligned} \quad (47)$$

- 4: At the $2j$ -th step $1 \leq j \leq \frac{n-1}{2}, \forall 1 \leq i_1 \leq \dots \leq i_{2j} \leq n$, if $\mathbf{x}_{i_{2j}}^* = 0$ define

$$\begin{aligned} \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}) &:= \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j-1}}) \oplus \mathbf{1}^{i_{2j}} \\ \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}) &:= \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j-1}}). \end{aligned} \quad (48)$$

If on the other hand, $\mathbf{x}_{i_{2j}}^* = 1$ define

$$\begin{aligned} \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}) &:= \mathbf{a}^l(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j-1}}) \\ \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j}}) &:= \mathbf{a}^r(\mathbf{x}^* \oplus \mathbf{1}^{i_1} \oplus \dots \oplus \mathbf{1}^{i_{2j-1}}) \oplus \mathbf{1}^{i_{2j}}. \end{aligned} \quad (49)$$

- 5: $\forall \mathbf{x}$, set
- 3)

$$\begin{aligned} \mathcal{P}(\mathbf{a}^l(\mathbf{x})|\mathbf{x}) &= \mathcal{P}(\mathbf{a}^r(\mathbf{x})|\mathbf{x}) = \frac{1}{2}, \\ \mathcal{P}(\mathbf{a}|\mathbf{x}) &= 0, \text{ otherwise.} \end{aligned} \quad (50)$$

6: **end procedure**



Device-Independent QKD against relativistic Eve

- The chained Bell inequalities $I_{AB}^{m, \text{ch}}$ are a family of two-party correlation Bell inequalities (XOR games) with m inputs and 2 outputs per party.

$$\mathcal{I}_{AB}^{m, \text{ch}} := \sum_{i=1}^m [\langle A_i B_i \rangle + \langle A_i B_{i+1} \rangle] \leq 2m - 2,$$

$$|\phi_+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

- QM: $I_{AB}^{m, \text{ch}} = 2m \cos(\pi/2m)$. NS: $I_{AB}^{m, \text{ch}} = 2m$.

$$A_i := \sin(\alpha_i)\sigma_x + \cos(\alpha_i)\sigma_z, \\ B_j := \sin(\beta_j)\sigma_x + \cos(\beta_j)\sigma_z.$$

$$\text{with } \alpha_i := \frac{\pi(2i-1)}{m} \text{ and } \beta_j := \frac{\pi(j-1)}{m} \text{ for } i, j = 1, \dots, m.$$

- In the limit $m \rightarrow \infty$, a perfect key bit between Alice and Bob is obtained (BHK, BCK, BKS) against the usual No-Signaling adversary. Underlying property: Monogamy of non-local correlations.

Proposition 4 ([39]). Any no-signaling distribution for which $\mathcal{I}_{AB}^{m, \text{ch}} < \mathcal{I}^*$ satisfies

$$P(A_k = a) \leq \frac{1}{2}(1 + \mathcal{I}^*), \\ P(B_l = b) \leq \frac{1}{2}(1 + \mathcal{I}^*),$$

$$\mathcal{I}_{AB}^{m, \text{ch}} + \langle KE_1 \rangle \leq 2m.$$

for all $a, b \in \{0, 1\}$ and $k, l \in [m]$.

$$I(B : E) \leq \mathcal{I}_{AB}^{m, \text{ch}}.$$

J. Barrett, A. Kent and S. Pironio, Phys. Rev. Lett. 97, 170409 (2006).

J. Barrett, L. Hardy and A. Kent, Phys. Rev. Lett. 95, 010503 (2005).

J. Barrett, R. Colbeck and A. Kent, Phys. Rev. A 86, 062326 (2012).



Device-Independent QKD against relativistic Eve

- In a Device-Independent framework, the relativistic causality conditions allow Eve to gain maximal information about the output key bit of such a protocol.
- Eve's observable is maximally correlated with the chosen observable of the honest parties even when algebraic violation is observed.

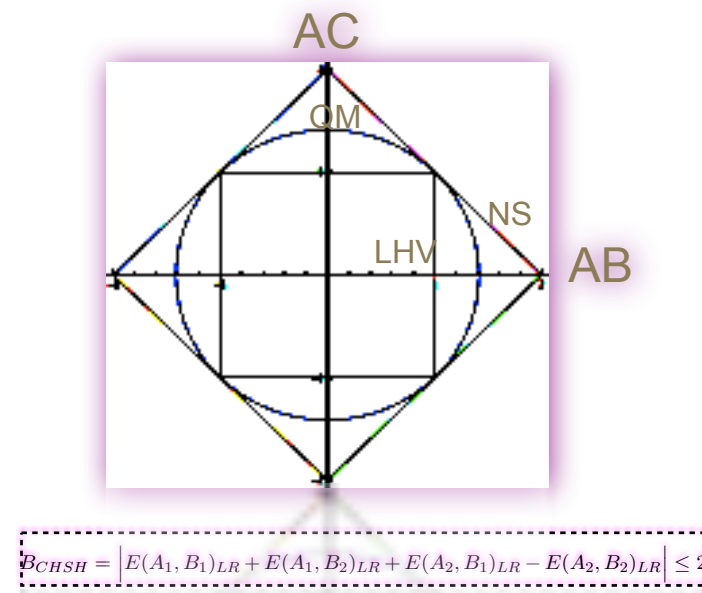
Proposition 3. Consider a three-party Bell scenario where Alice and Bob perform a test of the Braunstein-Caves chained Bell inequality $\mathcal{I}_{ch}^m$ (17) with an arbitrary number $m \geq 2$ of inputs per party and Eve measures a single observable E_1 . Suppose that in some inertial reference frame, the three space-like separated parties are arranged in 1-D, with $r_A < r_B < r_E$ and perform their measurements simultaneously, i.e., $t_A = t_B = t_E$. For any observable K of Bob, i.e., $K \in \{B_1, \dots, B_m\}$, there exists a relativistic causal box $\mathcal{P}(a, b, e|x, y, w)$ such that E_1 is perfectly correlated with K even when the algebraic violation of $\mathcal{I}_{AB}^{m, ch}$ is attained, i.e.,

$$\left[\mathcal{I}_{AB}^{m, ch} + \langle KE_1 \rangle \right]_{\mathcal{P}} = 2m + 1. \quad (20)$$



General properties of no-signaling theories

- **Monogamy:** Violation of CHSH Bell inequality by Alice-Bob precludes violation by Alice-Charlie.



Proposition 3. Consider a three-party Bell scenario, with Alice, Bob and Charlie each performing two measurements $x, y, z \in \{0, 1\}$ of two outcomes $a, b, c \in \{0, 1\}$ respectively. Suppose that in some inertial reference frame, the three space-like separated parties are arranged in 1-D, with $r_A < r_B < r_C$ and perform their measurements simultaneously, i.e., $t_A = t_B = t_C$. Then, there exists a three-party relativistically causal box $\mathcal{P}(a, b, c|x, y, z)$ such that

$$\langle CHSH \rangle_{AB} + \langle CHSH \rangle_{BC} = 8. \quad (19)$$



Genuine multipartite nonlocality

- Multiparty non-locality: Several classes of non-local correlations including Svetlichy S_2 -local, NS_2 -local, T_2 -local with $NS_2 \subset T_2 \subset S_2$.
- We introduce a new class of models C_2 :

Definition 5. Suppose that $P(a, b, c|x, y, z)$ can be written in the form

$$P(a, b, c|x, y, z) = \sum_{\lambda} q_{\lambda} P_{\lambda}(a, b|x, y) P_{\lambda}(c|z) + \sum_{\mu} q_{\mu} P_{\mu}(a, c|x, y, z) P_{\mu}(b|y) + \sum_{\nu} q_{\nu} P_{\nu}(b, c|y, z) P_{\nu}(a|x) \quad (28)$$

where the terms obey the relativistic causality constraints Eq.(12). Then the correlations $P(a, b, c|x, y, z)$ are said to be causal bi-local. Otherwise, we say that they are genuinely 3-way causal non-local.



Genuine Multiparty Nonlocality

- In the Bell scenario B(2,2,2) we give an inequality and quantum correlations obtained by suitable measurements on W-states that lead to its violation demonstrating genuine multiparty nonlocality.

$$0 \leq 6 - 2\langle A_1 B_1 \rangle - 2\langle A_2 B_1 \rangle - (1/2)\langle A_1 C_1 \rangle_{y=1} - (1/2)\langle A_1 C_1 \rangle_{y=2} + (1/2)\langle A_2 C_1 \rangle_{y=1} + (1/2)\langle A_2 C_1 \rangle_{y=2} - \langle A_1 B_2 C_1 \rangle \\ + \langle A_2 B_2 C_1 \rangle - (1/2)\langle A_1 C_2 \rangle_{y=1} - (1/2)\langle A_1 C_2 \rangle_{y=2} + (1/2)\langle A_2 C_2 \rangle_{y=1} + (1/2)\langle A_2 C_2 \rangle_{y=2} + \langle A_1 B_2 C_2 \rangle - \langle A_2 B_2 C_2 \rangle$$

$$|W\rangle = \frac{1}{\sqrt{3}} (|001\rangle + |010\rangle + |100\rangle).$$

$$A_i = \sin(\alpha_i)\sigma_x + \cos(\alpha_i)\sigma_z,$$

$$B_j = \sin(\beta_j)\sigma_x + \cos(\beta_j)\sigma_z,$$

$$C_k = \sin(\gamma_k)\sigma_x + \cos(\gamma_k)\sigma_z.$$

$$\mathcal{I}^{\text{qm}} \leq -0.67.$$

$$\alpha_1 = 4.51, \alpha_2 = -1.76, \beta_1 = 4.81, \beta_2 = 6.13, \gamma_1 = -1.13, \gamma_2 = 4.98.$$



Preferred Frame of Reference

- Consider superluminal influences in a preferred frame I at speed $u > c$.
- Fix (t_A, r_A) and (t_B, r_B) .
- Which (t_E, r_E) are allowed space-time region from which an Eve is able to influence correlations without violating causality?

Lemma 4. *Relativistic causality of the events A, B and E is satisfied if the following two conditions hold.*

- *Eve by her choice of input at E does not directly affect the individual statistics of the outcomes at points A and B separately.*
- *Eve by her choice of input at E is not able to signal to any space-time point S with $x_S := (t_S, r_S)$ via her modification of the joint distribution of the outcomes at A and B .*

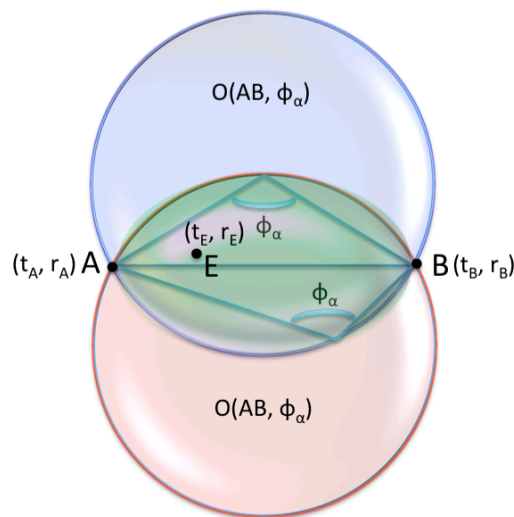


Preferred frame of reference

Theorem 7. Consider measurement events A, B with corresponding space coordinates $\mathbf{r}_A, \mathbf{r}_B$ in a chosen inertial reference frame I . Then a measurement event E can superluminally influence the correlations between A and B at speed $u > c$ without violating causality in I if and only if its space coordinate $\mathbf{r}_E$ satisfies

$$\mathbf{r}_E \in \text{Seg}(\bigcirc(AB; \varphi_\alpha)) \quad (39)$$

for any circle $\bigcirc$ with AB as a chord and having angle φ_α as the angle in the corresponding minor segment, where $\varphi_\alpha = \pi - 2 \arcsin(\alpha)$ and $\alpha = c/u$.



$$t'_A \geq t_A = t_E + \frac{|\mathbf{r}_A - \mathbf{r}_E|}{u}$$

$$t'_B \geq t_B = t_E + \frac{|\mathbf{r}_B - \mathbf{r}_E|}{u}$$

If we abandon the notion of a preferred frame, the regions transform.
Consequences are still Lorentz covariant.



Summary

- *Re-examined the derivation of the no-signaling constraints from causality.*
- **Implications in many directions, including quantum cryptographic and finite-superluminal explanations of quantum non-local correlations.**
- This work is supported by the John Templeton Foundation and ERC AdG grant QOLAPS.

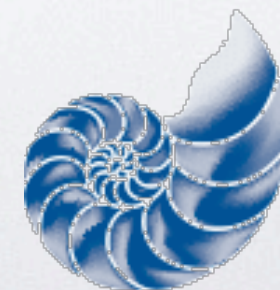


Summary and Open Questions

- Re-examine the ubiquitous no-signaling constraints from strict relativistic causality.
- Superluminal travel is logically perfectly possible as long as it leads to a consistent story that unfolds in time.
- “Non-local yet causal” theory that is different from Bohmian: allows for a notion of free-will.
- Open: “Extended quantum correlations” that obey the new constraints. Principles to rule out such correlations and dynamics.
- This work is supported by: John Templeton Foundation and ERC AdG grant QOLAPS.



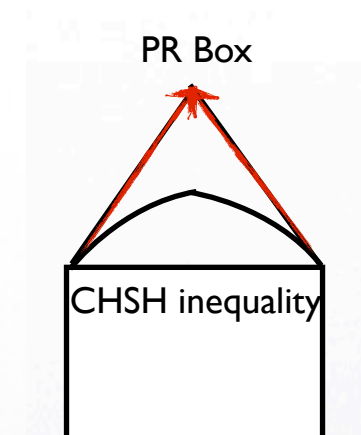
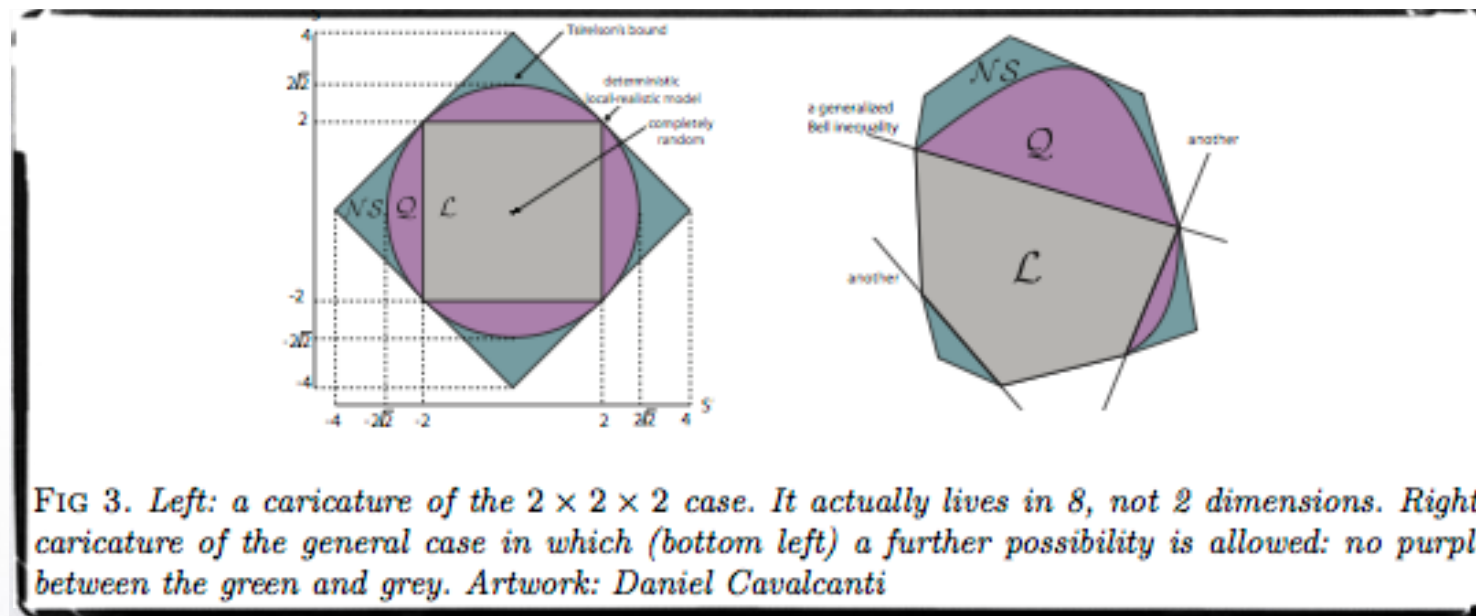
Thank you!



John
Templeton
Foundation



No-Signaling Polytope



- $LHV \subset Q \subset NS$.
- In the $B(2,2,2)$ scenario, non-local extreme box of NS is the PR box.

		$x_2 = 0$	$x_2 = 1$
	$a_2 \downarrow$	$a_2 = 0$	$a_2 = 1$
$x_1 = 0 \rightarrow$	$a_1 = 0$	1/2	0
	$a_1 = 1$	0	1/2
$x_1 = 1 \rightarrow$	$a_1 = 0$	1/2	0
	$a_1 = 1$	0	1/2

$a_1 \oplus a_2 = x_1 \cdot x_2$



- No signal carrying information can propagate faster than light - **No-Signaling Principle**.
 - Captured in the Bell scenario (n,m,k) by a set of constraints on the $P(a_1, \dots, a_n | x_1, \dots, x_n)$.
 - E.g. In the three party Bell scenario

$$\sum_{a_3} P(a_1, a_2, a_3 | x_1, x_2, x_3) = \sum_{a_3} P(a_1, a_2, a_3 | x_1, x_2, x'_3) \quad \forall a_1, a_2, x_1, x_2, x_3, x'_3$$

